NYS Forum

Information Security and Project Management
Communities of Practice

IS YOUR PROJECT VULNERABLE?

Reducing Security Risks with SSDLC

May 4, 2015
2:30 – 4:00

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

QED NATIONAL Problem Solved!

Is Your Project Vulnerable?

Reducing Security Risks with SSDLC

AGENDA:

- Introductions
- Presentations
- Panel Discussion and Q&A

Presenters and Panelists

Scott Rogler
NYS Office of
Information Technology Services

Russell Kiernan
QED
National

Deborah Snyder
NYS Office of
Information Technology Services

Nancy Mulholland
NYS Office of
Information Technology Services

Sara Holmberg
NYS Office of
Information Technology Services

Is Your Project Vulnerable?

Reducing Security Risks with SSDLC

Scott Rogler

Manager, Secure Systems Engineering

NYS Office of Information Technology Services

Enterprise Information Security Office

Building Security into Your Project

with New York States'

Secure Systems Development Life Cycle (SSDLC)

SSDLC – Secure by Design

Secure Systems Development Life Cycle (SSDLC)

- Building security into systems
- SSDLC toolkit to support security activities

SSDLC – Secure by Design

At MINIMUM, an SDLC contains the following security activities:

Define Security Roles and Responsibilities
Orient Staff to the SDLC Security Tasks
Establish a System Criticality Level
Classify Information
Establish Identity Assurance Level
Establish System Security Profile Objectives
Create a System Profile
Decompose the System
Assess Vulnerabilities and Threats
Assess Risks
Select and Document Security Controls
Create Test Data
Test Security Controls
Perform Certification and Accreditation
Manage and Control Change
Measure Security Compliance
Perform System Disposal

Is Your Project Vulnerable?

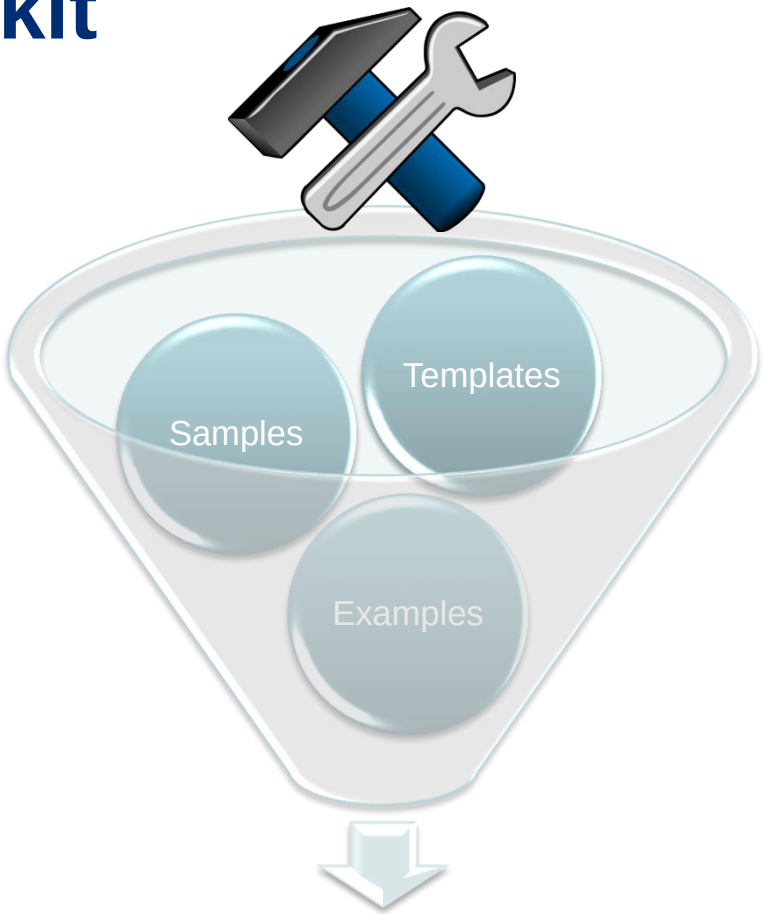
Reducing Security Risks with SSDLC

SSDLC – Secure by Design

NYS Secure Systems Development Lifecycle Standard (NYS-S13-001)

Project Management Life Cycle	Origination	Initiation & Planning Service Strategy	Execution Service Design / Service Transition / Service Operation		Closeout Continuous Improvement	
NIST SDLC Phases	N/A	Initiation	Acquisition / Development	Implementation / Assessment	Operations / Maintenance	Sunset (Disposition)
NYS PMG SDLC Phases	N/A	Initiation / Requirements Analysis / Design	Construction / Acceptance / Implementation			
Security activities within the SDLC		Risk Level / Initial Security Planning • Define security roles and responsibilities • Orient staff to the SDLC security tasks • Establish system criticality level • Classify information • Establish system identity assurance level • Establish system security profile objectives • Create a system profile • Decompose the system • Assess vulnerabilities and threats (preliminary) • Assess risks (preliminary) • Select and document security controls (preliminary)	Security Requirements and Controls • Assess vulnerabilities and threats (iterative) • Assess risks (iterative) • Select and document security controls	Security Testing, Documentation and C&A • Create test data • Test security controls • Measure security compliance • Document system security profile • Document security requirements and controls • Perform system certification and accreditation	Acceptance and Change Management • Measure security compliance (periodic) • Manage and control change • Perform system certification and accreditation (iterative)	Disposition Transition • Preserve information • Sanitize media • Dispose of hardware and software

SSDLC Toolkit



Security Plan
Documentation

Is Your Project Vulnerable?

Reducing Security Risks with SSDLC

Security Task

3	Initiation
10	Acquisition / Development
20	Implementation / Assessment
50	Operations / Maintenance

Is Your Project Vulnerable?

Reducing Security Risks with SSDLC

Russell Kiernan

Director, Management Consulting and
Information Security Services

QED National

A Secure SDLC Implementation

- Before Secure SDLC Implementation
- Drivers for Change
- Critical Success Factors
- The ‘After’ Picture

"Before" Secure SDLC

The Organization

- Industry
- Size
- Complexity

Information Security and SDLC

- Policies
- Standards
- Processes
- Practices
- Roles and Responsibilities

Drivers for Change

Changing Risk Profile

- Mergers
- Dramatically Increased Cybersecurity Threat
- Regulatory Environment

Needs

- Reduction of Complexity
- Efficient and effective process
- Demonstrate compliance

Critical Success Factors

- "Tone at the Top"
- Linkage to Enterprise Risk Management
- Clear Roles and Responsibilities
- Introduction of TISO role
- Awareness and training for ALL IT staff
- Info Security addressed directly in SDLC
  - Data Classification
  - Application Security Assessment
- Automation, Tools, and Dashboards
- Independent monitoring of compliance
- Effective risk identification and treatment

Outcome

- Implementation of Secure SDLC was completed and viewed as a success.
- ***BUT…***
  - Risk landscape changes rapidly.
  - Policies, Standards, Processes, Tools, etc. needed to be continuously reviewed and improved to address emerging risks.

Panel Discussion and Q&A

Scott Rogler
Manager, Secure Systems Engineering
NYS Office of Information Technology Services
Enterprise Information Security Office
Scott.Rogler@its.ny.gov

Russell Kiernan
Director, Management Consulting
and Information Security Services
QED National
(212) 481-6868
rkiernan@qednational.com

Deborah Snyder
Deputy Chief Information Security Officer
NYS Office of
Information Technology Services
Deborah.Snyder@its.ny.gov

Nancy Mulholland
CIO for Finance, Regulation and Gaming
NYS Office of
Information Technology Services
Nancy.Mulholland@its.ny.gov

Sara Holmberg
Manager, Governance, Portfolio and Strategy
NYS Office of
Information Technology Services
Sara.Holmberg@its.ny.gov

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

QED NATIONAL Problem Solved!